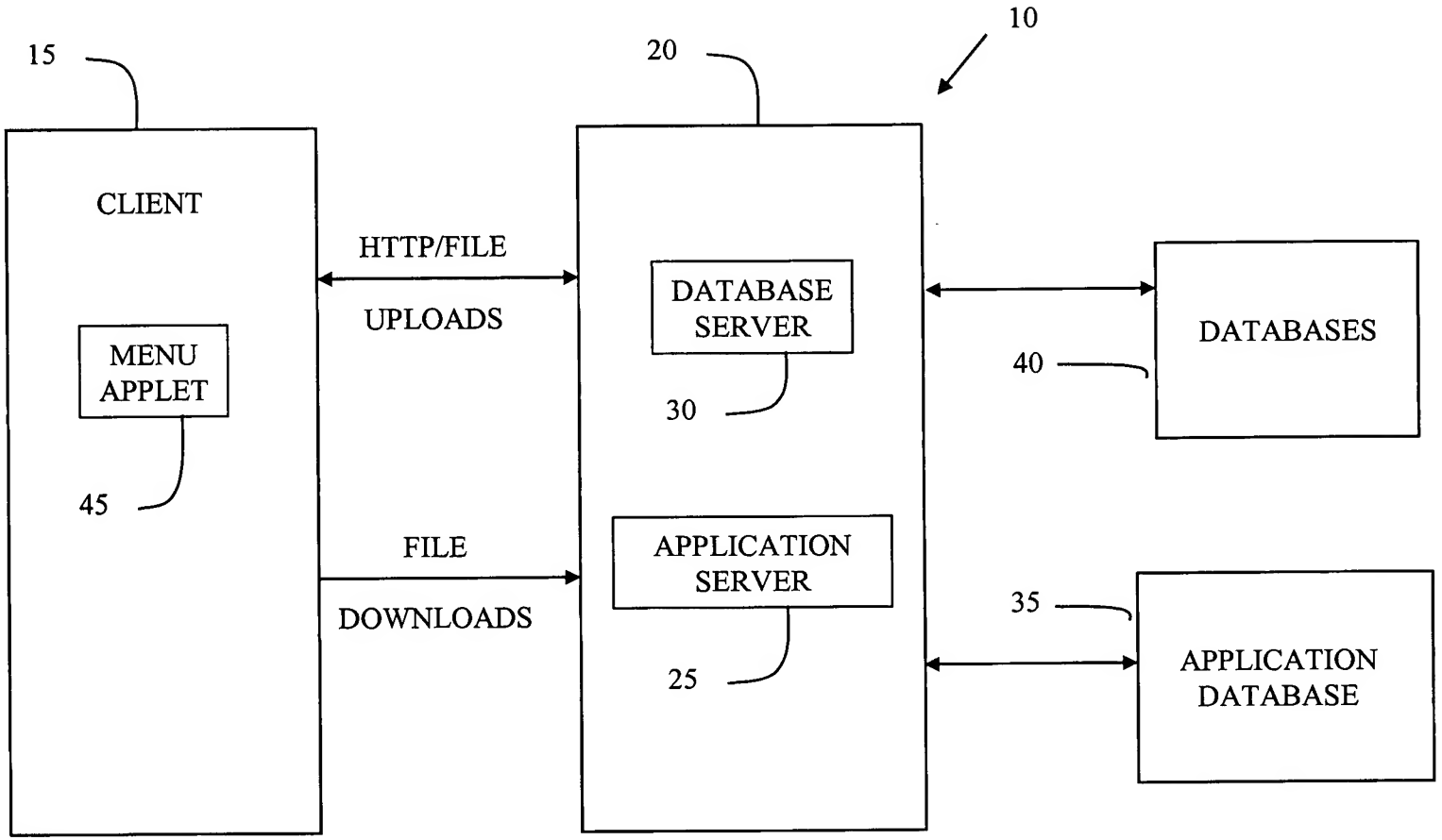
10
15
20
CLIENT
HTTP/FILE
UPLOADS
DATABASE SERVER
30
DATABASES
40
MENU APPLET
45
FILE
DOWNLOADS
APPLICATION SERVER
25
35
APPLICATION DATABASE

FIG. 1

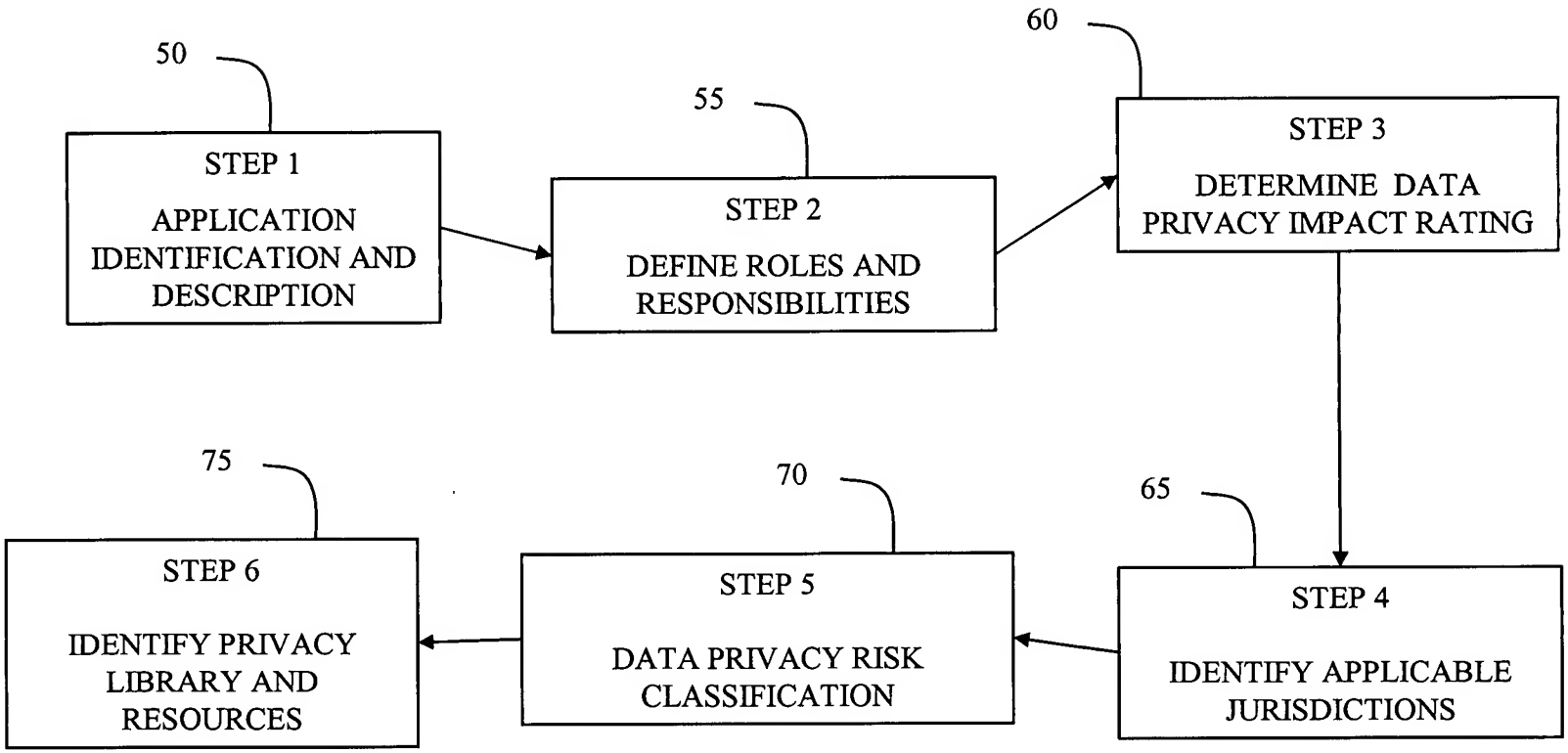
50
STEP 1
APPLICATION IDENTIFICATION AND DESCRIPTION
55
STEP 2
DEFINE ROLES AND RESPONSIBILITIES
60
STEP 3
DETERMINE DATA PRIVACY IMPACT RATING
65
STEP 4
IDENTIFY APPLICABLE JURISDICTIONS
70
STEP 5
DATA PRIVACY RISK CLASSIFICATION
75
STEP 6
IDENTIFY PRIVACY LIBRARY AND RESOURCES

FIG. 2

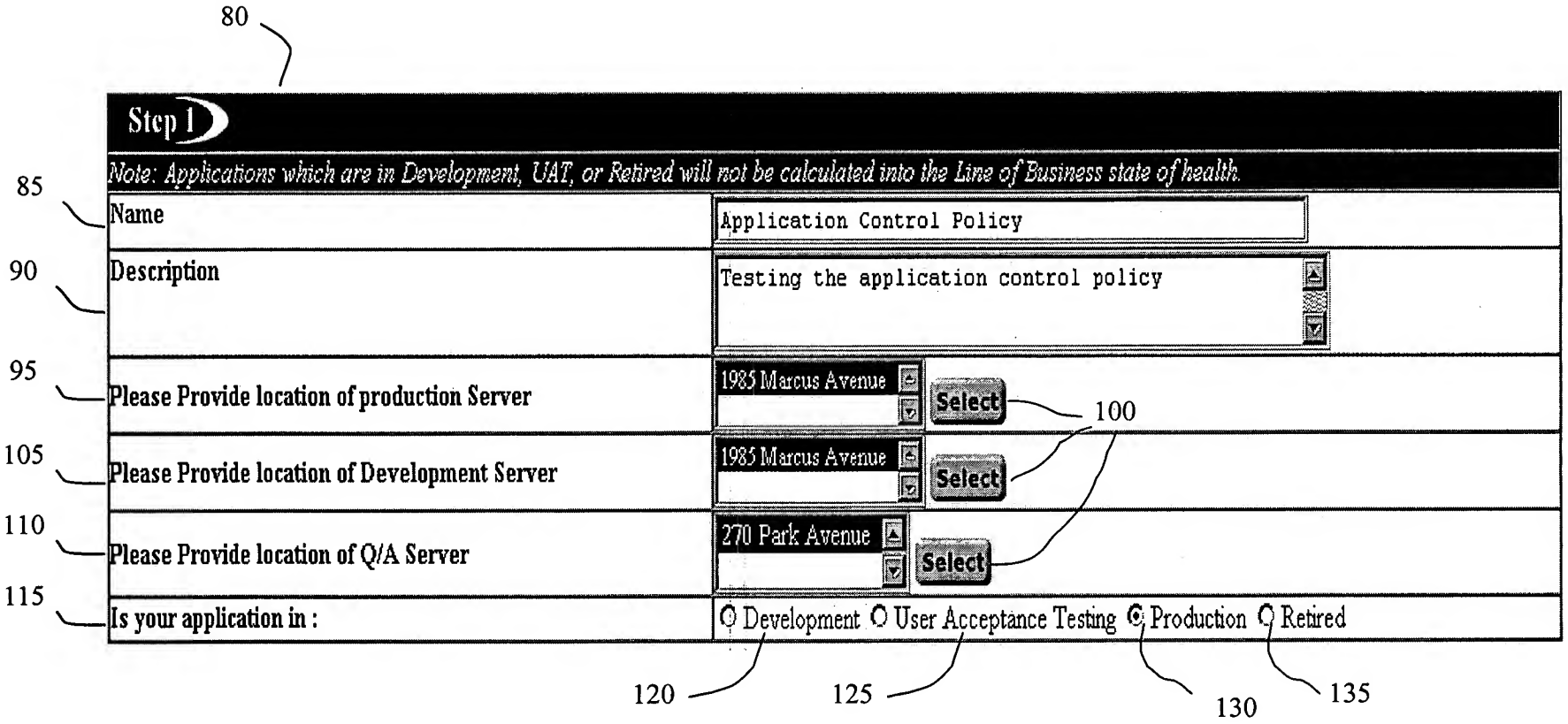
80
Step 1
Note: Applications which are in Development, UAT, or Retired will not be calculated into the Line of Business state of health.
85
Name
Application Control Policy
90
Description
Testing the application control policy
95
Please Provide location of production Server
1985 Marcus Avenue
Select
100
105
Please Provide location of Development Server
1985 Marcus Avenue
Select
110
Please Provide location of Q/A Server
270 Park Avenue
Select
115
Is your application in :
Development
User Acceptance Testing
Production
Retired
120
125
130
135

FIG. 3

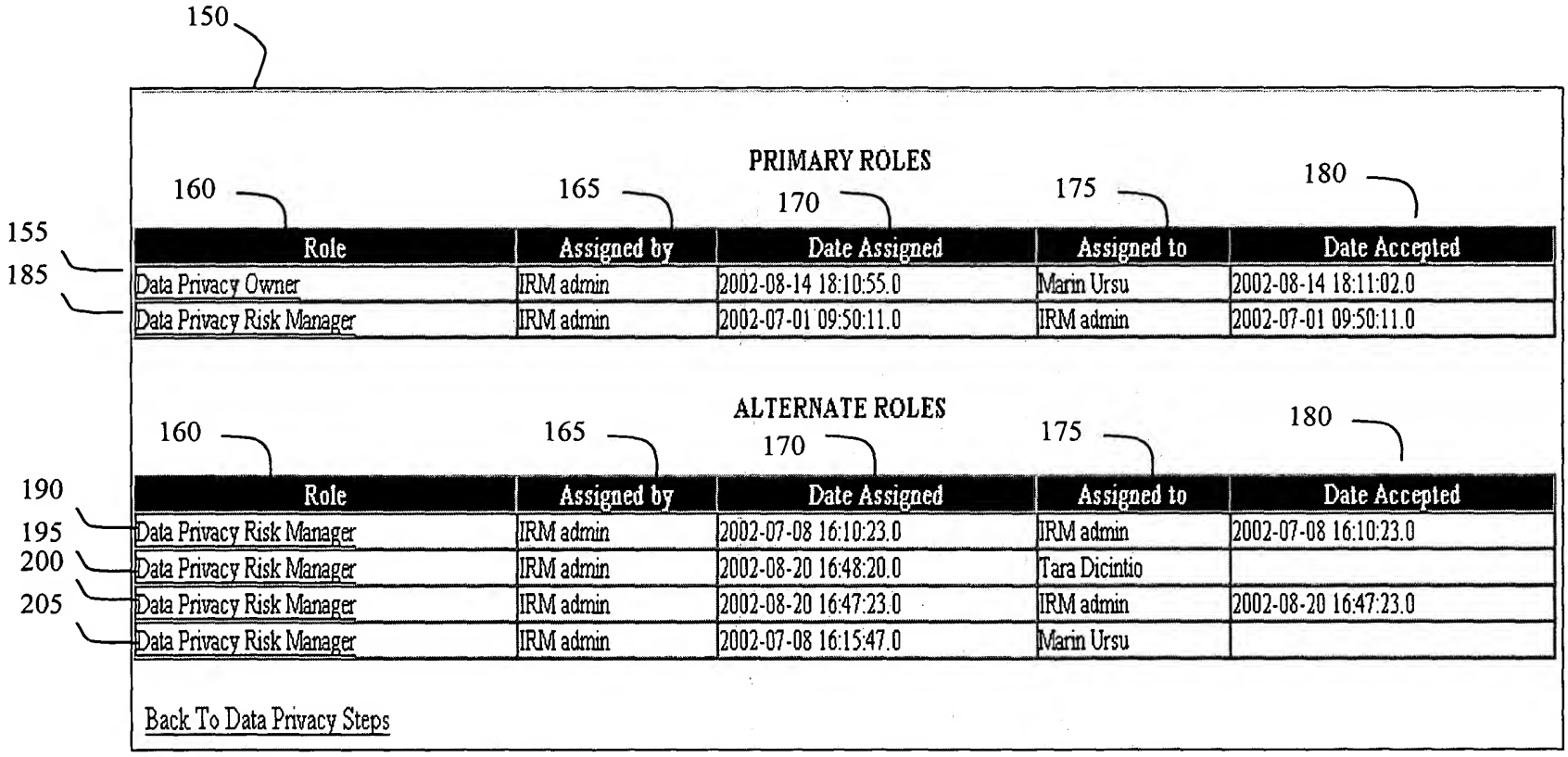
150
PRIMARY ROLES
160
165
170
175
180
155
185
Role
Assigned by
Date Assigned
Assigned to
Date Accepted
Data Privacy Owner
IRM admin
2002-08-14 18:10:55.0
Marin Ursu
2002-08-14 18:11:02.0
Data Privacy Risk Manager
IRM admin
2002-07-01 09:50:11.0
IRM admin
2002-07-01 09:50:11.0
ALTERNATE ROLES
160
165
170
175
180
190
195
200
205
Role
Assigned by
Date Assigned
Assigned to
Date Accepted
Data Privacy Risk Manager
IRM admin
2002-07-08 16:10:23.0
IRM admin
2002-07-08 16:10:23.0
Data Privacy Risk Manager
IRM admin
2002-08-20 16:48:20.0
Tara Dicintio
Data Privacy Risk Manager
IRM admin
2002-08-20 16:47:23.0
IRM admin
2002-08-20 16:47:23.0
Data Privacy Risk Manager
IRM admin
2002-07-08 16:15:47.0
Marin Ursu
Back To Data Privacy Steps

FIG. 4

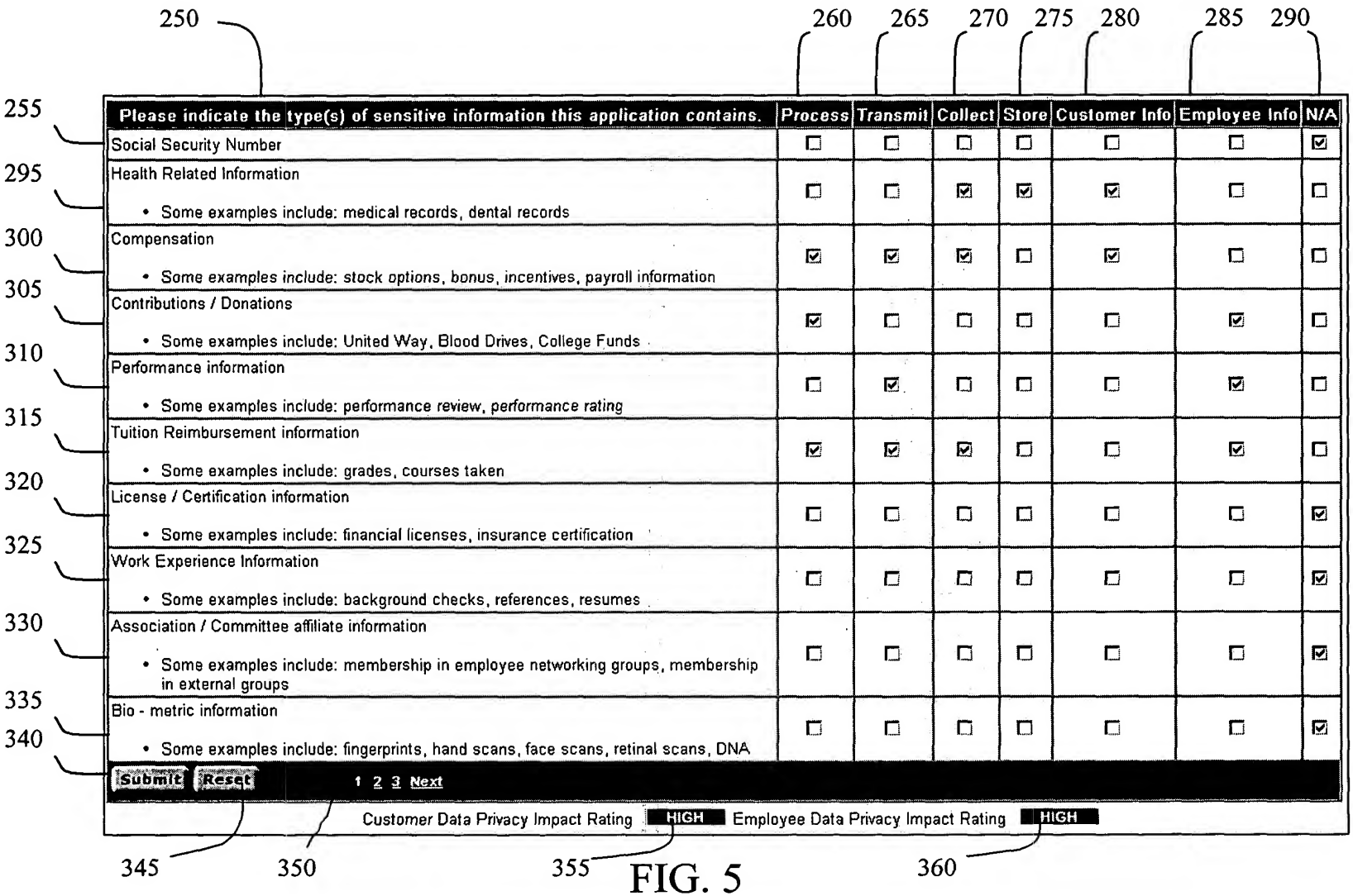
250
260
265
270
275
280
285
290
255
295
300
305
310
315
320
325
330
335
340
Please indicate the type(s) of sensitive information this application contains.
Process
Transmit
Collect
Store
Customer Info
Employee Info
N/A
Social Security Number
Health Related Information
• Some examples include: medical records, dental records
Compensation
• Some examples include: stock options, bonus, incentives, payroll information
Contributions / Donations
• Some examples include: United Way, Blood Drives, College Funds
Performance information
• Some examples include: performance review, performance rating
Tuition Reimbursement information
• Some examples include: grades, courses taken
License / Certification information
• Some examples include: financial licenses, insurance certification
Work Experience Information
• Some examples include: background checks, references, resumes
Association / Committee affiliate information
• Some examples include: membership in employee networking groups, membership in external groups
Bio - metric information
• Some examples include: fingerprints, hand scans, face scans, retinal scans, DNA
Submit
Reset
1 2 3 Next
Customer Data Privacy Impact Rating
HIGH
Employee Data Privacy Impact Rating
HIGH
345
350
355
360

FIG. 5

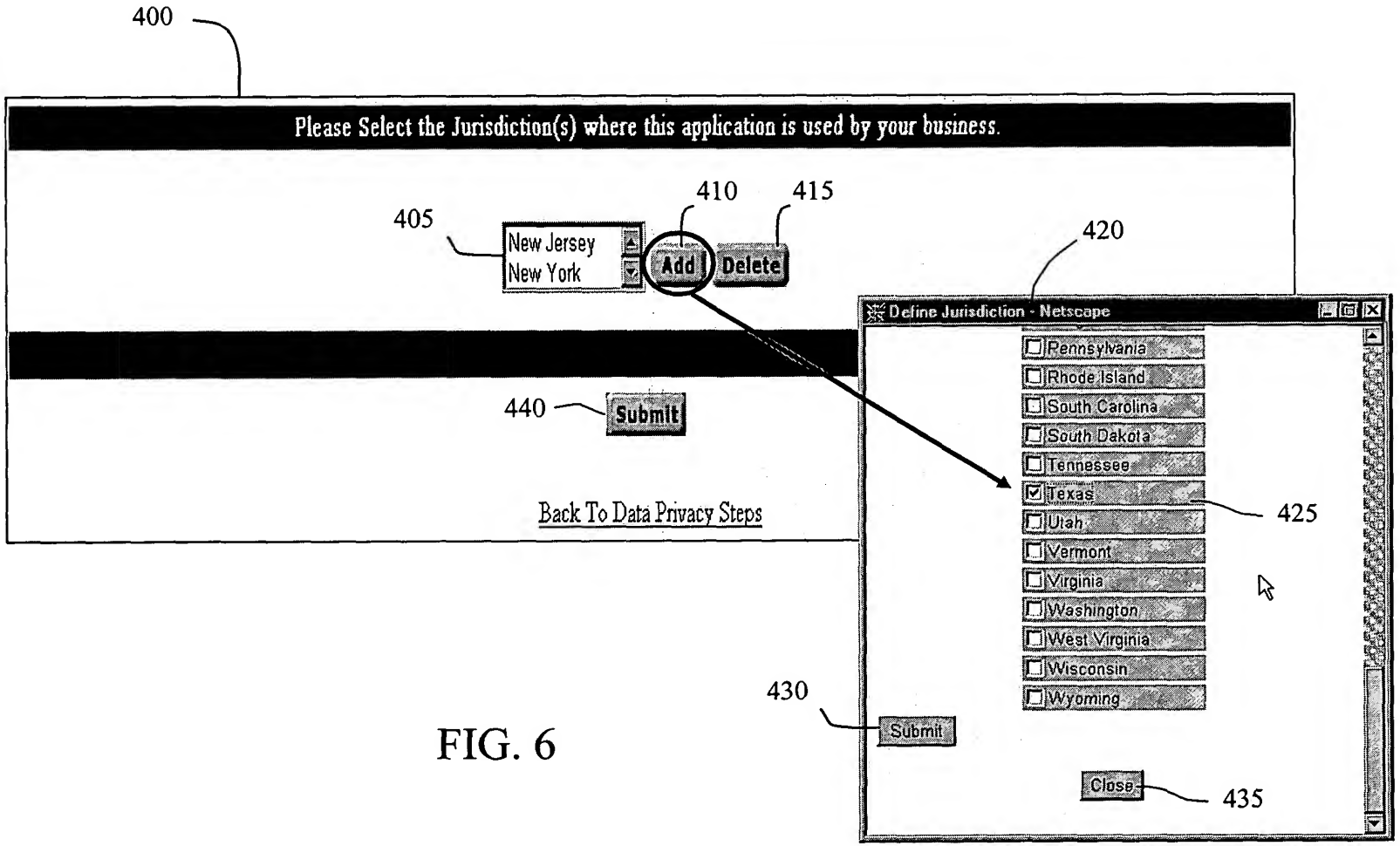
400
Please Select the Jurisdiction(s) where this application is used by your business.
405
New Jersey
New York
410
Add
415
Delete
420
Define Jurisdiction - Netscape
Pennsylvania
Rhode Island
South Carolina
South Dakota
Tennessee
Texas
Utah
Vermont
Virginia
Washington
West Virginia
Wisconsin
Wyoming
425
440
Submit
Back To Data Privacy Steps
430
Submit
Close
435

FIG. 6

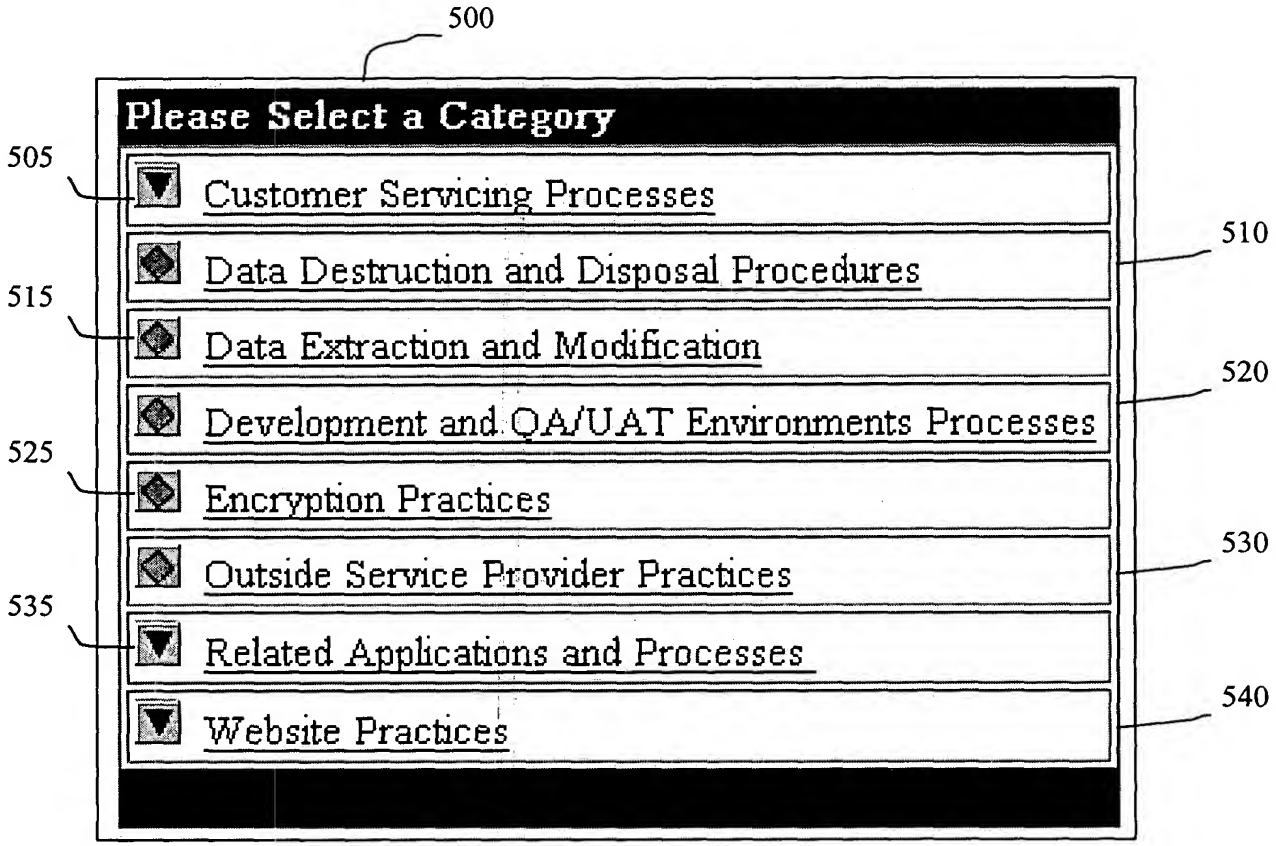
500
Please Select a Category
505
Customer Servicing Processes
510
Data Destruction and Disposal Procedures
515
Data Extraction and Modification
520
Development and QA/UAT Environments Processes
525
Encryption Practices
530
Outside Service Provider Practices
535
Related Applications and Processes
540
Website Practices

FIG. 7

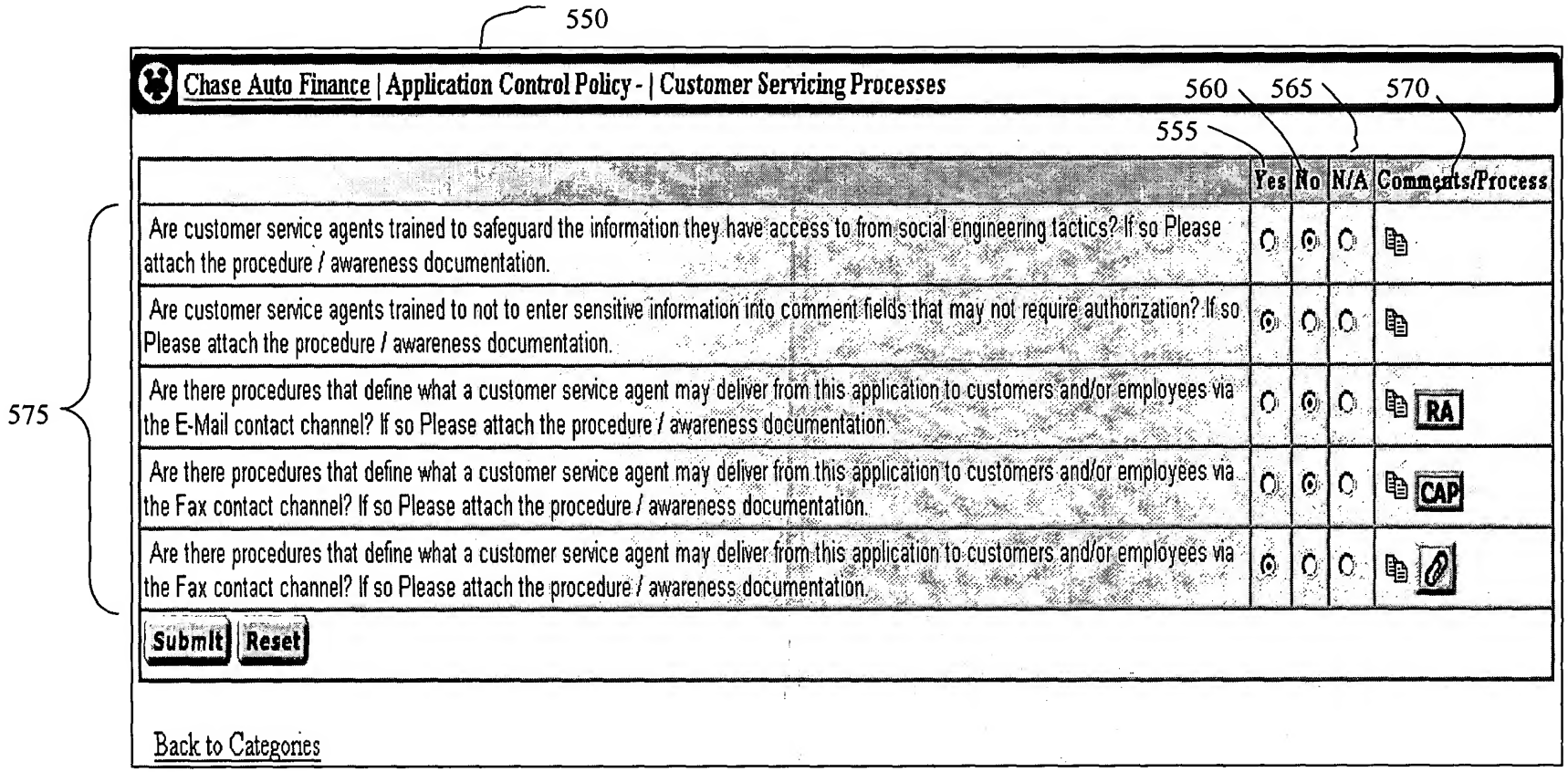
550
Chase Auto Finance | Application Control Policy - | Customer Servicing Processes
560
565
570
555
Yes
No
N/A
Comments/Process
Are customer service agents trained to safeguard the information they have access to from social engineering tactics? If so Please attach the procedure / awareness documentation.
Are customer service agents trained to not to enter sensitive information into comment fields that may not require authorization? If so Please attach the procedure / awareness documentation.
Are there procedures that define what a customer service agent may deliver from this application to customers and/or employees via the E-Mail contact channel? If so Please attach the procedure / awareness documentation.
RA
Are there procedures that define what a customer service agent may deliver from this application to customers and/or employees via the Fax contact channel? If so Please attach the procedure / awareness documentation.
CAP
Are there procedures that define what a customer service agent may deliver from this application to customers and/or employees via the Fax contact channel? If so Please attach the procedure / awareness documentation.
575
Submit
Reset
Back to Categories

FIG. 8

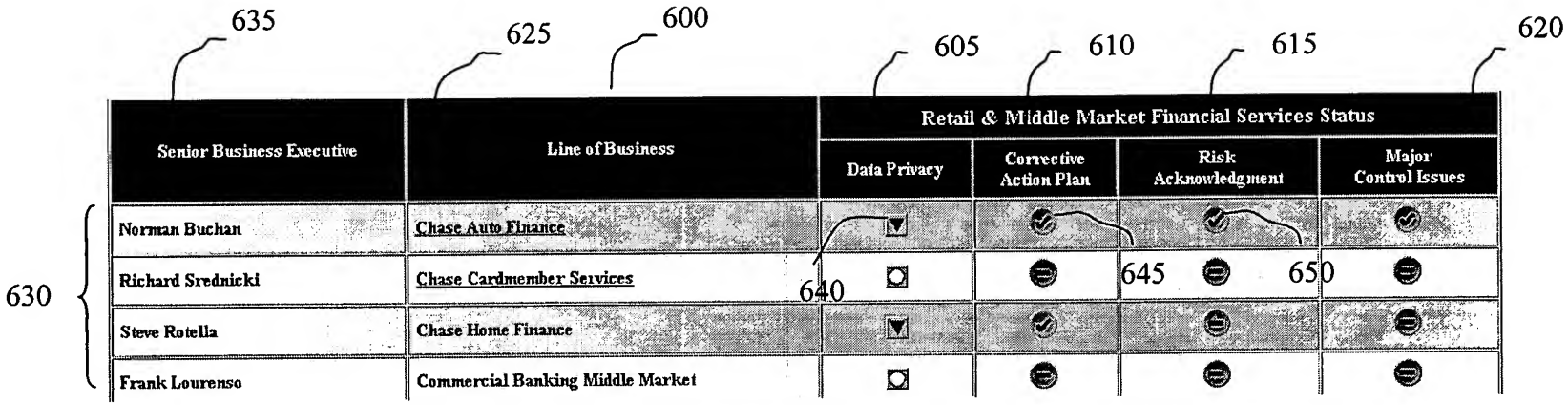
635
625
600
605
610
615
620
Senior Business Executive
Line of Business
Retail & Middle Market Financial Services Status
Data Privacy
Corrective Action Plan
Risk Acknowledgment
Major Control Issues
Norman Buchan
Chase Auto Finance
Richard Srednicki
Chase Cardmember Services
Steve Rotella
Chase Home Finance
Frank Lourenso
Commercial Banking Middle Market
630
640
645
650

FIG. 9

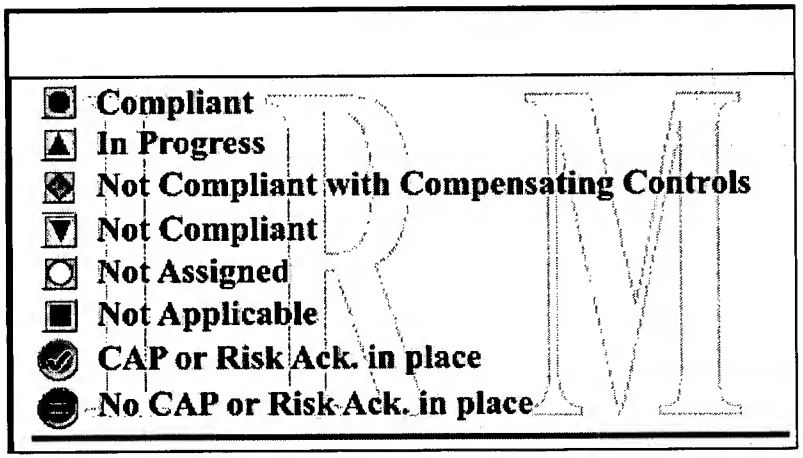
Compliant
In Progress
Not Compliant with Compensating Controls
Not Compliant
Not Assigned
Not Applicable
CAP or Risk Ack. in place
No CAP or Risk Ack. in place

FIG. 10

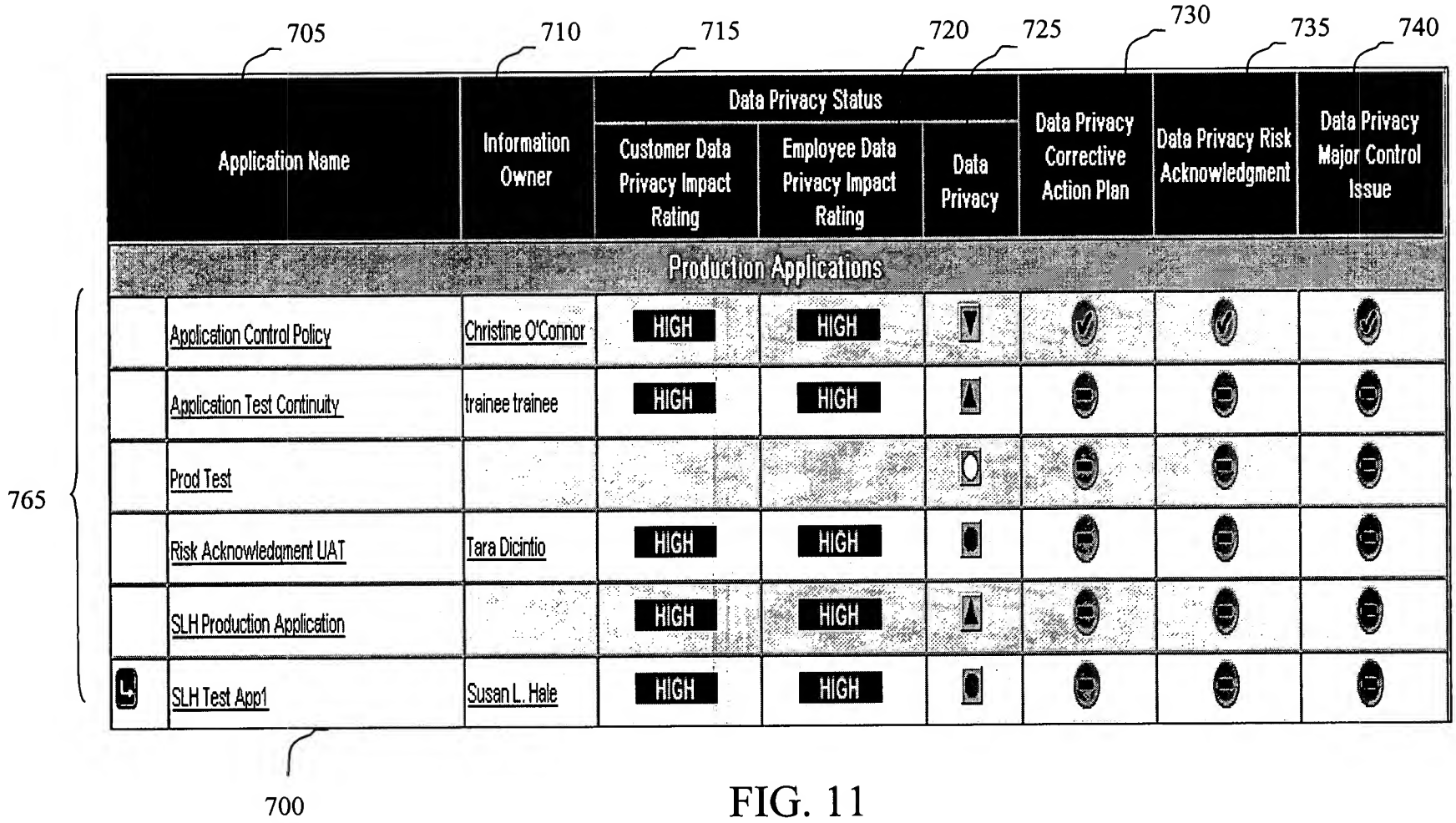
705
710
715
720
725
730
735
740
Application Name
Information Owner
Data Privacy Status
Customer Data Privacy Impact Rating
Employee Data Privacy Impact Rating
Data Privacy
Data Privacy Corrective Action Plan
Data Privacy Risk Acknowledgment
Data Privacy Major Control Issue
Production Applications
Application Control Policy
Christine O'Connor
HIGH
HIGH
Application Test Continuity
trainee trainee
HIGH
HIGH
Prod Test
Risk Acknowledgment UAT
Tara Dicintio
HIGH
HIGH
SLH Production Application
HIGH
HIGH
SLH Test App1
Susan L. Hale
HIGH
HIGH
765
700

FIG. 11

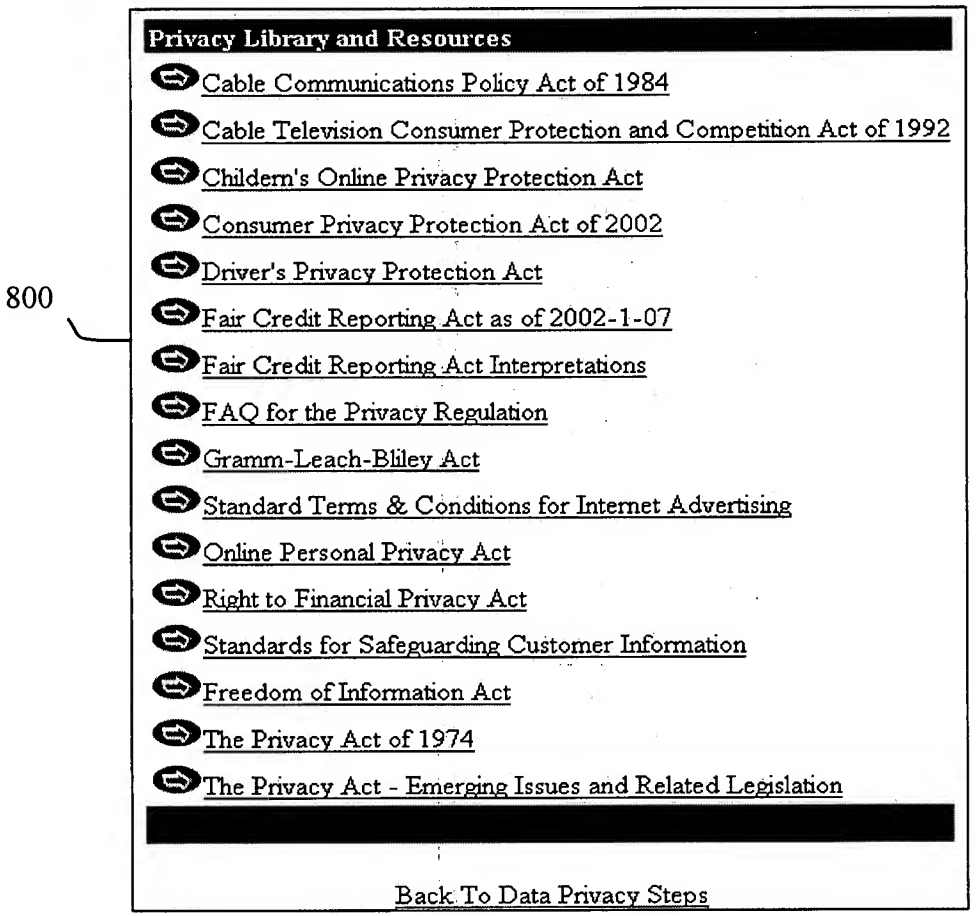
800
Privacy Library and Resources
Cable Communications Policy Act of 1984
Cable Television Consumer Protection and Competition Act of 1992
Childern's Online Privacy Protection Act
Consumer Privacy Protection Act of 2002
Driver's Privacy Protection Act
Fair Credit Reporting Act as of 2002-1-07
Fair Credit Reporting Act Interpretations
FAQ for the Privacy Regulation
Gramm-Leach-Bliley Act
Standard Terms & Conditions for Internet Advertising
Online Personal Privacy Act
Right to Financial Privacy Act
Standards for Safeguarding Customer Information
Freedom of Information Act
The Privacy Act of 1974
The Privacy Act - Emerging Issues and Related Legislation
Back To Data Privacy Steps

FIG. 12